

Re: A Question of Permutations of Vectors of Bits

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-07/2198.html>

From: David Wagner (daw_at_mozart.cs.berkeley.edu)

Date: 07/31/03

Date: Thu, 31 Jul 2003 06:17:55 +0000 (UTC)

Simon G Best wrote:

> P is a permutation of $2n$ -bit vectors. x and y are $2n$ -bit vectors, such that

> $y = x + P(x)$

> (where '+' is bitwise-xor). P is easily invertible.

>

> [P is] a bijective mapping of $2n$ -bit vectors to $2n$ -bit vectors; a

> permutation such as a block cipher's encryption function with a

> particular key.

Ahh. Then I think this problem is hard. More precisely, I believe it is hard if P behaves like a random permutation[1], which ought to be the case if there are no weaknesses in the key schedule or structure of the block cipher.

Indeed, if it were too easy to solve your problem, then I think there would be shortcut inversion and collision attacks on Davies-Meyer hashing.

Special case: If $y=0$, then you're looking for fixpoints of P . In some cases, you can exploit the cipher's structure to find the fixpoints of encryption under a specified key. (Of course, when this is possible, it means that P does not behave like a random permutation.)

[1] In a sense analogous to random oracles (rather than to pseudorandom functions, PRFs).